commpact

User Manual

For quick user information please refer to the CommPact
Quick User Guide provided on our website: www.electronics-line.com

UPGRADING
EVERYDAY
SECURITY

Quick Reference Guide

Function	Press...	Additional Information
ARM	OR OR	**One-Key Arming is disabled on the Control System, enter your user code when arming.**
	FULL PART PERIMETER	**The default master code is 1234.**
INSTANT ARM	**Hold down this key until "Instant Arming OK?" is displayed. Then Press .**	**Instant arming cancels the entry delay after Part or Perimeter arming. This feature can be enabled by your installer.**
DISARM	**[USER CODE]**	**Entering your user code also silences the siren in the event of an alarm.**
PANIC ALARM		**Press these buttons together and hold them down to generate an alarm.**
FIRE ALARM		
MEDICAL ALARM	+	
MENU MODE	**then [USER CODE]**	**Use the menu navigation buttons (▲/▼) until the required menu item is displayed then press ✓. Alternatively, enter the shortcut (e.g. 21 for Bypass Zones).**
CHECK TROUBLE CONDITIONS	**Use this key scroll the system trouble list**	**Pressing ▼ also silences any trouble tones that may be sounded by the system.**
SWITCH PGM ON	**then 30**	**Enter 30 for PGM.**
SWITCH PGM OFF		
SERVICE CALL	+	**"Dialing" is displayed. The number dialed for the service call is programmed by your installer.**
GLOBAL CHIME	**then**	**Use the menu navigation buttons (▲/▼) to choose enable or disable, then press ✓.**
RECORD MESSAGE		**After recording a message, "Message Waiting" is displayed until the message is played back.**
PLAY MESSAGE	**then**	**The Message Center is an optional feature that is included with certain versions of CommPact Control System.**

Telecontrol Commands

Function	Press...
2-WAY AUDIO	2
FULL ARM	3
DISARM	6

Function	Press...
CANCEL SIREN	9
EXTEND CALL	7
DISCONNECT	* then #

Table of Contents

Quick Reference Guide ..... **ii**

Table of Contents ..... **iii**

1. Introduction and Overview **1**
1.1. Documentation Conventions 1
1.2. Security System Components 2
1.3. System Monitoring 3
1.4. Self-Monitoring 3
1.5. Telephone Control 3
1.6. Vocal Message Annunciation 4
1.7. Web/Smartphone Access 4

2. The User Interface **5**
2.1. Front Panel 5
2.2. Alarm Sounding Patterns 7
2.3. Keyfobs 8
2.4. Wireless Keypads 8

3. Arming and Disarming **10**
3.1. Arming Modes 10
3.2. Arming the System 10
3.3. Disarming the System 12
3.4. Arm Status and Other System Status Indication 12
3.5. Arming Tones 13
3.6. Remote Arming/Disarming 14

4. Panic Alarms **16**
4.1. Keypad Alarms 16
4.2. Keyfob Panic Alarm 17
4.3. Medical/Panic Emergency 17

5. PGM Control **18**
5.1. Keyfob Control 18
5.2. Telephone Control 18
5.3. SMS Control 18

6. Telecontrol **20**
6.1. Calling your Home 20
6.2. Service Call 22
6.3. Two-Way Audio after an Alarm 22
6.4. Two-Way Audio Follow-Me 22
6.5. Simplex Mode 22

7. Advanced System Operation **23**
7.1. Cancel Report 23
7.2. Zone Bypassing/Unbypassing 24
7.3. User Codes 24
7.4. Follow-Me 26
7.5. Event Log 26
7.6. Service Menu 27

Appendix A: Menu Structure **32**
Appendix B: Web User Application **33**
Register to MyELAS 33
Login to MyELAS 35
The Main Page 36
Arming and Disarming 38
Web Application Settings 39
Event Log History 48
Appendix C: Glossary **49**

1. Introduction and Overview

This user manual explains all you need to know about your **CommPact** security system and provides step-by-step instructions for all the system's user functions. In addition to the explanation you will receive from your installer, we urge you to read this manual so that you can take full advantage of your system's features. Keep this manual in an accessible location for future reference.

The **CommPact** system has many features in order to suit a wide range of applications. This manual outlines all of these features but it is likely that there are options that are not relevant to your system. If you have any questions regarding the availability of the features described in the manual, please ask your installer.

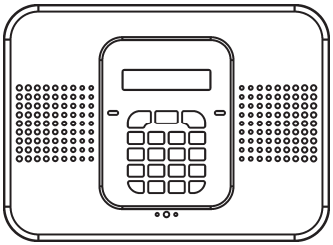
1.1. Documentation Conventions

In order to simplify the procedures that appear in the rest of this manual, the following conventions are used:

Item...	Description...
Select...	Use the arrow buttons to scroll through the options and press ✓.
From the Event Log Menu, select Clear Log.	Enter the main menu by pressing ✓and entering your user code. Using the arrow buttons, navigate until you reach Event Log and press ✓. Using the arrow buttons, navigate until you reach Clear Log and press ✓.
From the Service menu, select Set Time/Date, Set Date.	The same as above only this time you are navigating through three menu levels.
[7012]	The shortcut to a specific menu item from the main menu. In this case, this is the shortcut for Set Date. These appear in the procedures as an additional aid to menu navigation.
[#5]	A shortcut to a specific item in a sub-menu. For example, [#5] is the shortcut to Bell enable disable in the sub-menu that is opened once you have selected the detector you want to program.
✓, ▲buttons	buttons that appear on the keypad ( )
5. Interface Test	The text that actually appears on the LCD display (italics).
	Note
	Important caution, please pay attention.

1.2. Security System Components

Your security system is made up of a Control System, various detectors and a number of optional peripheral devices. This section explains the role of each component in your system.



Control System

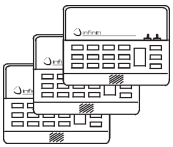
The Control System is the brain of the system. It communicates with all the devices connected to the system. For example, in the event of a burglary, a detector sends a signal to the Control System indicating that it has sensed motion on the premises. On receiving this signal, the Control System makes the decision to report the alarm to your monitoring service and activate the siren.

Detectors

Detectors are the devices that protect your home, alerting the Control System when there is a breach in security. Magnetic contacts protect your doors and windows while motion detectors are able to detect an intruder moving across its field of view. Vibration and glassbreak detectors are able to sense low-amplitude vibrations and forced break-in attempts around vulnerable access points. Additionally, smoke, carbon monoxide, gas leak and flood detectors can be installed to provide an early warning in the event of a fire, the presence of dangerous gases or the potential for flooding.

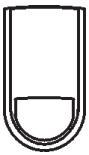
Keyfobs

Keyfobs are hand-held transmitters that are used to operate the system. Various keyfobs are available providing a number of functions. For example, arming/disarming the system and sending panic and medical assistance alarms.



Keypads

The keypads enable you to communicate with the Control System in order to perform a number of different functions. The main function you can perform using a keypad is to arm the system when leaving your home and to disarm on your return.

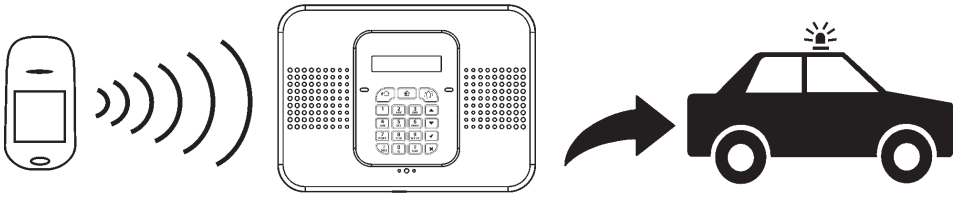


Sirens and Strobes

While the Control System includes a built-in internal siren, it is possible that you also have an external siren and strobes installed. The sirens are sounded and the strobes are activated during certain alarm conditions serving to warn you and ward off intruders.

1.3. System Monitoring

When an event occurs within the system, the Control System sends a message to your monitoring service describing the exact nature of the event. This enables the monitoring service to take the required action. System monitoring can implement either regular telephone or cellular communication.



A detector detects. ▸ ▸ ▸ The Control System is alerted. ▸ ▸ ▸ An alarm is generated and the monitoring service is notified.

IMPORTANT: There is a communication delay of 30 seconds in this Control System for non-fire alarms. This delay can be reduced to 15 seconds or it can be increased to 45 seconds at the option of the end user in consultation with the installer. Fire, gas and flood alarms are communicated immediately.

1.4. Self-Monitoring

In addition to the ability to report to a monitoring service, the system can also send you and other users notification when an event occurs. This may be in the form of vocal messages played over the telephone or, if your system supports cellular communication, you can receive information on system status via SMS. If an alarm occurs on the premises, you are informed no matter where you are in the world.

1.5. Telephone Control

DTMF Telecontrol

The **CommPact** offers a range of "Telecontrol" features that provide remote access via the telephone (PSTN or Cellular). These features include remote arming/disarming, PGM output activation/deactivation, siren cancel and Two-Way audio via the Control System's built-in microphone and speaker – see p.20, 6 Telecontrol.

The Two-Way Audio features allow you to contact your home directly in the event of an alarm or simply to check your home while you are away.

SMS Control

Using your cellular phone, you can also send SMS commands to arm/disarm the system, to turn on/off the PGM output, and get confirmation when the command is received. – see p.13, 3.5 Arming Tones.

1.6. Vocal Message Annunciation

Vocal message annunciation is an optional feature that, if enabled in programming, causes the system to play short messages that indicate system status.

1.7. Web/Smartphone Access

The Web/Smartphone application provides an interface to your security system from your Internet browser or Smartphone. You can perform a wide range of tasks such as arm/disarm, zone bypass, and user code management. Additionally, you can set up the contacts whom you wish to be alerted (by email or text message) when selected events occur.

The Web/Smartphone application also allows you to check your home at any time either by viewing a history of recent events that have occurred. For further information, see p. 33, Appendix B: Web User Application.

2. The User Interface

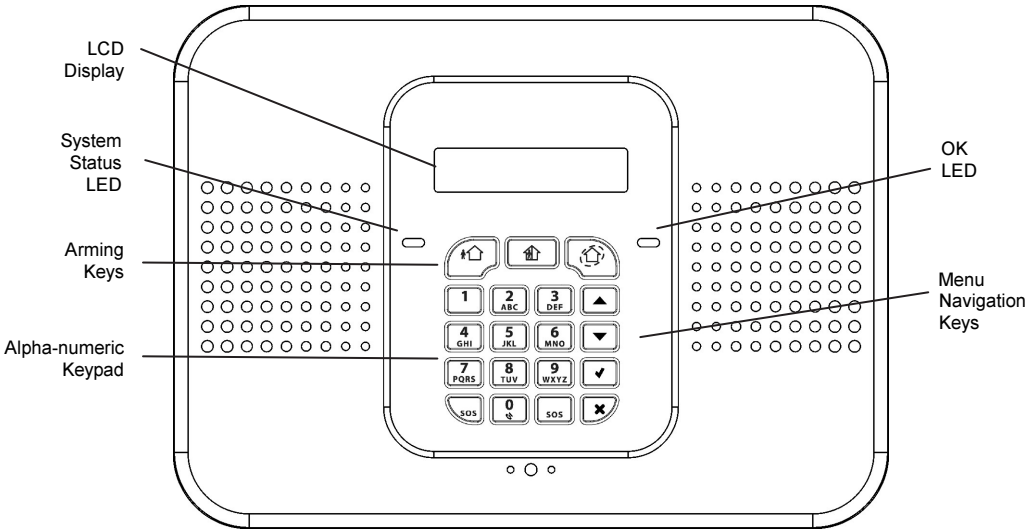
There are several methods you can use to operate the system. Apart from the keypad on the front panel, your system may include a number of peripheral devices such as keypads and keyfobs.

This chapter provides a brief introduction to each of the devices you can use to operate the system. It is important that you familiarize yourself with these devices before reading the following chapters that describe system operation in further detail.

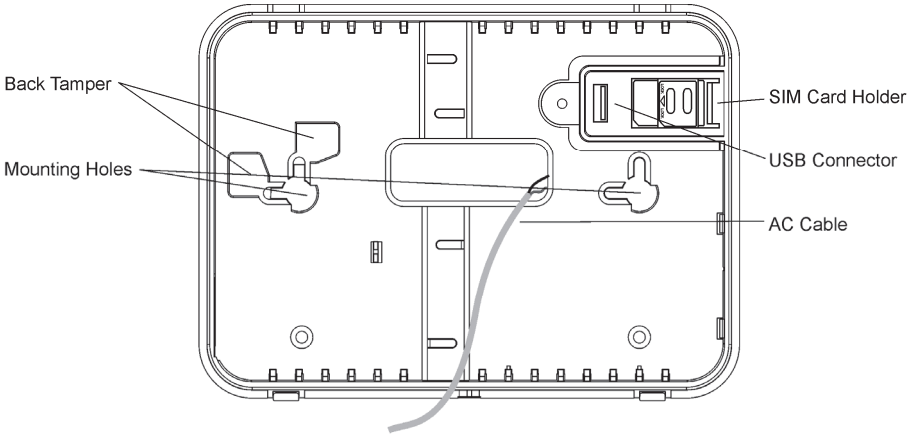
The front panel is the main user interface that provides you with all the functions you need to control your security system.

2.1. Front Panel

LCD Front Panel display and LEDs inform you of system arming status, power failures, and system trouble conditions. Its alphanumeric keypad enables you to enter your user code when arming and disarming, and to silence the siren in the event of an alarm.



Next diagram shows the Control System's back panel that provides access to the SIM card and the USB Connector.



Arming Keys

Three arming keys are available: Full, Part, and Perimeter. These buttons arm the system using one of the three arming methods. One-key Arming is an option that is programmed by your installer.

Service Call Button

The Service Call button enables you to contact the monitoring service and talk to an operator.

To initiate a service call, press the up arrow button ▲, then press and hold down the Service Call button 0.

Vocal Message Recording and Playback

Front Panel allows you to record a short message that may be played back later by another user – see p. 27, 7.6. Service Menu, Message Center.

System Status LEDs

The System Status indicators provide essential information on the status of the system such as arm, disarm, alarm and power failure conditions.

OK LED Status	**Meaning**
Off	Both AC and Battery power are disconnected.
On Green	System Power status is OK and there is no System Trouble.
Flashing Green	Open Zone. Check that the windows and doors are closed and no movement is detected by the detectors within the protected area.
On Yellow	System Trouble.

OK LED Status	**Meaning**
Flashing Yellow (slow)	Battery low from the Control System or transmitters.
Flashing Yellow (fast)	AC loss.
Flashing Yellow (intermittent)	System Trouble in addition to AC loss/Low Battery.

LED Status	**Meaning**
Off	The system is disarmed.
On Green	The system is armed.
Flashing Red	An alarm has occurred. Alarm indication is cleared the next time you arm the system or view the relevant arming event in the event log.

Alarm indication is not displayed after a silent panic alarm.

System Trouble Indication

In the event that the system detects a trouble condition, "System Trouble" appears on the display. To identify the problem, scroll through the trouble list by pressing ▼. Scrolling the trouble list also silences system trouble tones that may be sounded if enabled in programming. When the trouble condition is restored, it is removed from the system trouble list.

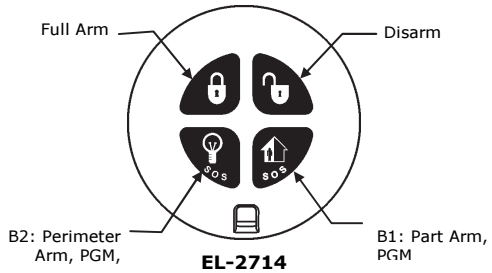
2.2. Alarm Sounding Patterns

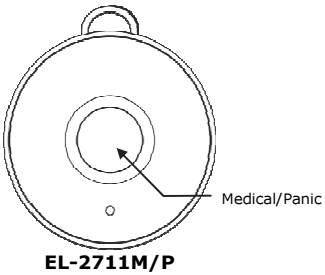
The following table summarizes various alarms sounded by the control system.

Alarm	**Alarm Sounding Pattern Description**
Burglary	ON (continuously)
Fire	ON - ON - ON, 1.5-second pause, ON - ON – ON.....
Gas	ON - ON - ON - ON (short bursts), 5 second pause, ON - ON - ON - ON.....
Medical	ON (continuously) – only applicable for Medical alarm from zone
Flood	4 rapid tones sounded once per minute (same as Trouble tones)
Environmental	

2.3. Keyfobs

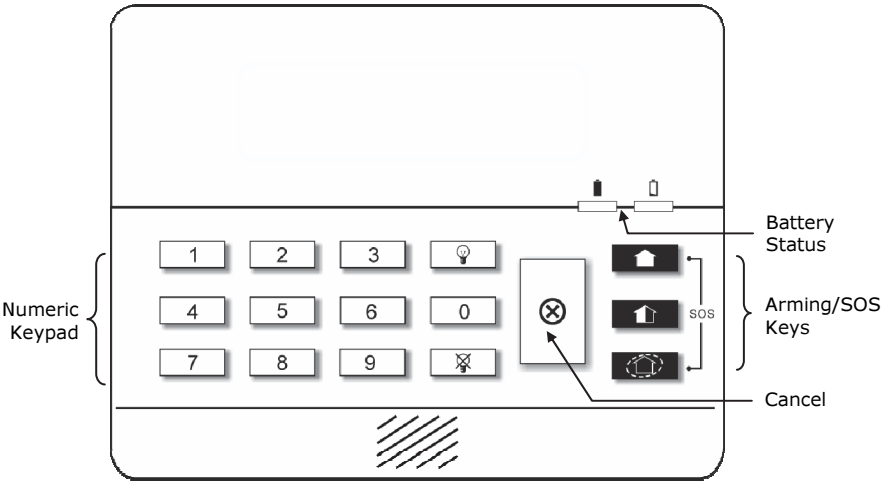
The **CommPact** supports up to nineteen keyfob transmitters. The functions of the buttons on each keyfob are shown in the examples below.





2.4. Wireless Keypads

The system supports up to four wireless keypads. You can use the keypad (EL-2620) as an arming station, and generate a panic alarm in the event of emergency.



Numeric Keypad

The numeric keypad allows you to arm or disarm the system by entering a user code.

Arming Keys

Three arming keys are available: Full, Part and Perimeter. These keys arm the system using one of the three arming methods. One-key Arming is an option that is programmed by your installer. If this option is disabled, you must also enter a user code when arming.

Panic Alarm

Simultaneously pressing the Full and Perimeter buttons generates a panic alarm.

Cancel

The Cancel key clears the keypad in the event that you pressed a key by mistake.

For example, when entering your code you enter a wrong digit, the system waits for you to enter all four digits before it decides that the code is incorrect. Pressing the Cancel key causes the keypad to disregard what was previously entered enabling you to start again.

Battery Status LEDs

Every time a key is pressed, one of the Battery Status LEDs is lit. When the battery needs to be replaced, the red Low Battery LED is lit.

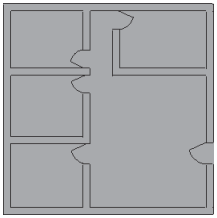
3. Arming and Disarming

Arming can be defined as activating the system. When the system is armed, it monitors the zones that are protected by the detector. If a detector senses an intrusion, the system generates an alarm.

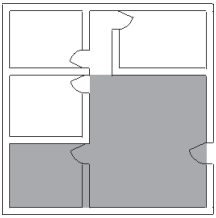
3.1. Arming Modes

Three arming modes are available: Full, Part and Perimeter. These modes enable you to arm your system accordingly to suit different circumstances.

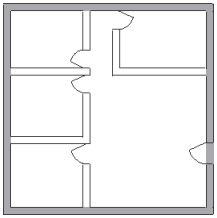
You can only disarm all the active arming modes.



Full Arming
Full arming activates the entire system. This arming method is used when you intend to leave your home, leaving the premises empty.



Part Arming
This arming method enables you to arm a section of your home while remaining on a different part of the premises.



Perimeter Arming
Perimeter arming enables you to activate the perimeter zones (the windows and doors of your home) enabling you to move freely within the protected area.

Certain detectors, such as smoke, carbon monoxide, gas and flood detectors, are always active regardless of system status.

3.2. Arming the System

Before arming the system, check that all doors and windows are secured so that the system is ready for arming.

Arming with the Keypad

To arm the system using the front panel/wireless keypads:

- Press one of the three arming keys, the exit delay begins to count down. At the end of the exit delay, the system is armed.

Arming with the Keyfob

The default functions for B1 is part arming and for B2 -- perimeter arming.

To arm the system using the keyfob:

- Press the relevant button/buttons on your keyfob (see below); the exit delay begins to count down. At the end of the exit delay, the system is armed.

Combination arming

There is an option to activate two arming modes simultaneously.

The possible combinations are:

- Full + perimeter
- Part + Perimeter

For combination arming, activate the first arming mode, and, while the exit delay of the first arming mode is counting down, activate the second arming mode. It is not important which arming mode you choose first.

It is not possible to activate Full and Part arming modes simultaneously.

It is necessary to disarm first when changing from one arming mode to another arming mode.

Forced Arming

Forced arming enables you to arm when the system is not ready. For example, if a door protected by a magnetic contact is open, you may arm the system on condition that the door will be closed by the end of the Exit delay. If the door is still open after the exit delay expires, an alarm is generated.

Forced arming is available only if the option is enabled in programming.

Instant Arming

Instant arming is a feature that allows you to cancel the entry delay after Part or Perimeter arming the system. For this feature to function, it must be enabled in programming by your installer.

To instantly arm the system.

1. Check if the system is ready to arm.
2. Press the Part or Perimeter arming button on the keypad (enter your user code if required).
3. Press and hold down ▲ on your keypad until the message *Instant Arming, OK?* is displayed
4. Press ✓; the entry delay for the current arming period is canceled.

Supervised Arm

Supervised Arm is an optional feature designed to supervise intrusion detector activity before you arm the system.

If Supervised Arm is enabled in programming and the system has not received a transmission from a detector for a certain amount of time, all arming methods that include that detector shall not be available.

In this case, press ▼ to check which detector is causing the "System Not Ready" condition. To make the required arming method available, activate the detector. If activating the detector does not help, there may be a problem with the detector. You can bypass the faulty detector's zone to allow system arming until the problem is remedied – see p. 24 7.2. Zone Bypassing/Unbypassing.

Motion detectors have a three or four minute delay between transmissions.

3.3. Disarming the System

When you enter the premises, the entry delay begins to count down. You must disarm the system within the entry delay time to prevent the system from triggering an alarm.

To disarm the system using a keypad:

- Enter your user code.
  The system is disarmed.

You can only disarm all the active arming modes.

To disarm the system using a keyfob:

- Press the disarm button.

3.4. Arm Status and Other System Status Indication

The following table explains the various arm status descriptions as they appear on the LCD display.

DISARMED
12:22:11

Status	Meaning
DISARMED	The system is disarmed.
FULL ARMED	The system has been armed using the displayed arming method.
PART ARMED	

Status	Meaning
PERIMETER ARMED	
PART ARMED INST	
PERIM ARMED INST	
FULL ARMING	The system is in the process of arming using the displayed arming method (displayed during exit delay).
PART ARMING	
PERIMETER ARMING	
PART ARMING INST	
PERI ARMING INST	

The system may be programmed to display arm status at all times or only for the first two minutes or 30 seconds after you arm or disarm the system.

In addition to arm status, the system displays messages on statuses that may prevent you from arming your system (see the following table):

Status	Meaning
ZONES IN ALARM	Zones have been violated.
TAMPER ALARM	The system has been tampered with.
SYSTEM NOT READY	The system is not ready to arm, check that all doors and windows are closed.
KEYPAD LOCKED	Five unsuccessful attempts were made to enter a user code; the keypad is locked for 30 minutes. If this message appears, it is still possible to arm/disarm the system using a keyfob. Arming is possible using a keypad if one key arming is enabled.
SYSTEM TROUBLE	A trouble condition has been detected, press ▼ for further details.

3.5. Arming Tones

Arming tones are the chimes that the system sounds during the entry/exit delay and when the system arms or disarms. Various options are available that determine the pattern of these tones.

Arming tones may be sounded by either the external wireless siren or the control panel's built-in siren.

3.6. Remote Arming/Disarming

Remote Arming/Disarming via SMS

You can arm and disarm the system remotely by sending SMS commands from a cellular phone.

Each SMS command contains the following elements:

- SMS Command Descriptor (up to 43 characters of free text)
- # (separates the descriptor from the actual command)
- User Code
- Command ((120=Disarm, 121=Full Arm, 122=Part Arm, 123=Perimeter Arm, 124=Full + Perimeter Arm, 125=Part + Perimeter Arm, 200 = Arm Status*)

The following example shows the format of an SMS command for disarming the system:

SMS Command Descriptor							User Code				Command		
D	I	S	A	R	M	#	1	2	3	4	1	2	0

While the SMS Command Descriptor is optional, you must start the SMS command with the # symbol for the system to accept the command. Don't use "#" symbol within the descriptor text.

Arm Status Reply

On receiving an Arm Status request message (see command "200" above), the system returns a status message to the sender. This message includes the system status and the descriptor of the user or the device used to arm/disarm the system.

The following example shows an Arm Status Reply message reporting that the system was fully armed by Master User.

F	U	L	L		A	R	M	E	D	-	M	A	S	T	E	R		U	S	E	R

SMS Confirmation message

After an SMS command is executed by the system, if programmed by your installer, a confirmation message may be returned to your mobile phone. The following example shows the confirmation message you receive for the sample command from the previous section.

D	I	S	A	R	M	E	D

* Master code is required for the Arm Status command.

Remote Arming/Disarming via the Telephone

Using the Telecontrol feature, you can arm and disarm the system via the telephone. For further information on the Telecontrol features, see p. 20, 6. Telecontrol.

Remote Arming/Disarming via WUAPP and WAP

You can arm and disarm the system remotely using the WUAPP (Web User Application) and WAP – see Appendix B: Web User Application.

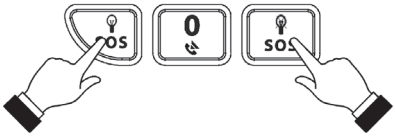
4. Panic Alarms

Panic alarms enable you to send a message to the monitoring service in the event of an emergency. There are various types of panic alarm and several methods you can use to generate them.

4.1. Keypad Alarms

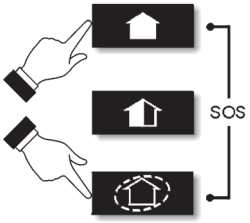
To activate an SOS Panic Alarm from the front panel keypad:

- Press and hold down the SOS buttons simultaneously.



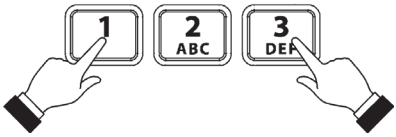
To activate an SOS Panic Alarm from the Wireless keypad (see p. 8, 2.4 Wireless Keypad):

- Press and hold down the Full and Perimeter buttons simultaneously.



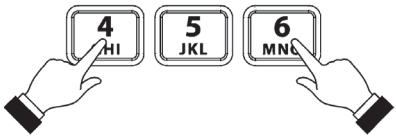
To activate a Fire alarm from the front panel keypad:

- Press and hold down buttons 1 and 3 simultaneously.



To activate a Medical alarm from the front panel keypad:

- Press and hold down buttons 4 and 6 simultaneously.



4.2. Keyfob Panic Alarm

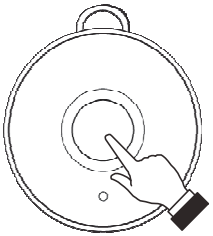
To activate a Panic alarm using the four-button keyfob (EL-2714):

- Press the lower two buttons simultaneously.

4.3. Medical/Panic Emergency

The one-button keyfob (EL-2711M) is designed to send a message to your monitoring service in the event of a medical/panic emergency.

The transmitter is water-resistant and can be worn around the neck as a pendant.



5. PGM Control

PGM is a programmable output that is triggered according to specific system status conditions, or by remote command sent via PSTN, GSM, Ethernet, keyfob, or Remote Programmer as explained below.

PGM programmable output can be controlled (using the keyfobs, remotely by telephone or SMS) or programmed to react to specific system status conditions. For example, PGM can be programmed to switch on when the system is armed or when a specific zone is triggered.

How PGM reacts to the On command is determined by the installer in programming. PGM can be programmed to switch on until the Off command is received/the end of status condition that turned it on.

5.1. Keyfob Control

You can control PGM using the four button keyfob registered to the system. This option can be programmed by the installer. See p. 8 2.3. Keyfobs.

5.2. Telephone Control

Using the Telecontrol feature, you can control PGM output remotely via the telephone. For further information on the Telecontrol features, see p. 20, 6. Telecontrol.

5.3. SMS Control

If your system supports cellular communication, you can control PGM via your mobile phone using a number of SMS commands. The SMS commands are designed to be entered as templates on your mobile phone.

Each SMS command contains the following elements:

❶ SMS Command Descriptor (up to 43 characters of free text)

❷ # (delimiter – separates the descriptor from the actual command)

❸ User Code (4 digits)

❹ Command (0=Off, 1=On)

❺ Device Number (30 for PGM output)

The following example shows the format of an SMS command to switch PGM On.

❶									❷	❸				❹	❺	
P	G	M		O	N				#	1	2	3	4	1	3	0

Do not include the symbol '#' in the descriptor as the system regards any text after this symbol as part of the command. The SMS Command Descriptor is optional but you must still enter the '#' before the user code.

SMS Confirmation Message Format

After an SMS command is executed by the system, if programmed by your installer, a confirmation message may be returned to your mobile phone. This message includes the PGM descriptor and the command that was sent. The following example shows the confirmation message you receive for the sample command from the previous section.

P	G	M		O	N

6. Telecontrol

The **CommPact** Control System offers a range of Telecontrol features that provide remote access via the telephone. These features include Two-Way Audio, remote arming/disarming and siren cancel.

Two-Way Audio

You may use the Two-Way Audio features to check your home in the event of an alarm or as an alternative means of communicating with members of your family. For example, you may wish to call an elderly person who has difficulty reaching the phone. Using its Two-Way Audio features, the Control System automatically picks up the call and you can communicate via its built-in microphone and speaker.

6.1. Calling your Home

You may call your home at any time in order to contact your family, operate your system or check your home while you are away. This feature is available for both regular telephone communication and cellular communication.

Making a Call using a Regular Telephone

When your security system shares a telephone line with other devices (e.g. telephone handsets, an answering machine or fax), it is important that the Control System distinguish between calls so that it knows when to pick up the relevant call. For this purpose the **CommPact** employs a double call method.

To make a call to the Control System using the double call method:

1. Dial your telephone number.
2. Wait for two or three rings then hang-up.
3. Wait at least five seconds and dial the number again; on the second ring, the Control System picks up and sounds two tones.

Making a Cellular Call to the System

If your system supports cellular communication, it has its own individual telephone number. Therefore, the double call method is not necessary and you may call the Control System directly.

Call Procedure

To prevent unauthorized attempts to call your Control System, you must enter a user code when calling your home – see p. 25, 7.3. User Codes, Code 29.

To call your home:

1. Call the Control System either using the double call method or directly (see above); when the Control System picks up, two tones are sounded.
2. Enter the telecontrol code (Code 29) on your telephone within 15 seconds.

⚠ **Do not enter your user code until you hear the two tones. Any digits entered before the tones are sounded are disregarded by the system.**

3. A tone is sounded to indicate that the system is ready to receive commands. The following commands are available:

- Press "**2**" for Two-Way Audio.
  If the TWA mode is defined as "Simplex" (see p. 22 6.5. Simplex Mode.), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "**1**" on your telephone. To switch back to Listen mode, press "**0**" on your telephone.

  ☞ During the TWA session, you can adjust the speaker volume using the arrow buttons.
- Press "**3**" to fully arm the system.
- Press "**430**" to activate PGM output (Unit 30)
- Press "**530**" to deactivate PGM output (Unit 30)
- Press "**6**" to disarm the system.
- Press "**9**" to cancel the siren.

☞ The Arm/Disarm, PGM on/off, and Siren canceling can also be executed at any time during a Two-Way Audio session.
Error beeps (three tones) sound in case of a wrong command.
To clear the last command, press "*" or "#".

4. The duration of the call is an option programmed by your installer. Ten seconds before the end of the call, two short tones are sounded. To extend the call, press "**7**" on your telephone.
5. To disconnect before the end of the call, press "*" then "#" on your telephone.

Siren Muting

The siren is muted during Two-Way Audio communication. At the end of the call, the siren is re-activated (if the Siren Cut-Off has not yet expired). You can cancel the re-activation of the siren by pressing "9" on your telephone during the call.

6.2. Service Call

The Service Call feature enables you to call the monitoring service.

To make a Service Call:

- Press and hold down the up arrow button and then press and hold Service Call button for a few seconds.

If using Simplex mode, the call is connected in Listen mode – see p. 22 6.5. Simplex Mode.

6.3. Two-Way Audio after an Alarm

In the event of Burglary, Fire, Gas Detection, Flood and Medical alarms, the Control System is able to report the events and then stay on the line. This allows the monitoring service to verify the alarm or provide assistance in the event of an emergency.

6.4. Two-Way Audio Follow-Me

This feature causes the Control System to call you in the event of an alarm so that you may check your family and home.

When the Control System calls, you will hear two short tones when you pick up the phone. Press "2" on your telephone to answer the call.

If you press “9” to answer the call, the Control System simultaneously cancels the siren when you answer the call.

If using Simplex mode, the call is connected in Listen mode – see p. 22 6.5. Simplex Mode.

6.5. Simplex Mode

It is possible that the Two-Way Audio features on your system are programmed to operate in “Simplex” mode. Simplex mode means that one party may speak while the other party listens.

If using Simplex mode, the call is connected in Listen mode. In Listen mode, the microphone on the Control System is turned on so that you can listen in. If you want to switch to Speak mode, press “**1**” on your telephone.

In Speak mode, the microphone is turned off and the speaker is turned on so that you can speak to the person on the other end of the line. If you want to switch back to Listen mode, press “**0**” on your telephone.

7. Advanced System Operation

Besides the basic functions described in the previous chapters, you can access additional functions via the menu. This chapter describes these functions and the menu navigation procedure.

Menu Navigation

Using the LCD keypad on the front panel, you can navigate through the menus using the menu navigation buttons (▲/▼) and make simple yes/no decisions using the ✓and ✘buttons.

The availability of menu items depends on the user code that you used to enter Menu mode. Some menu items are limited to the master code only (User 1). Certain menu items, such as system programming functions, are not intended for the user and can only be accessed by the installer.

The following example explains the procedure for Event Log viewing (master code access only).

1. Press ✓ to enter Menu mode.
2. Enter the master code; the first menu item in the main menu, *1. Cancel Report* is displayed.
3. Press ▼ until *6. Event Log* is displayed.
4. Press ✓ to enter the Event Log menu; *1. View Log* is displayed.
5. Press ✓ to choose the displayed item.

Press ✘if you do not want to choose the displayed item. Pressing ✘also takes you back to the previous menu level.

Menu mode automatically terminates two minutes after the last keystroke.

Throughout this chapter, we have tried to include all of the system functions using a similar structure and order as they appear in the menu.

7.1. Cancel Report

The Cancel Report function enables you to prevent the system from reporting in the event of a false alarm.

To cancel report:

- From the main menu, select Cancel Report [1]; all pending messages to the monitoring service are canceled.

7.2. Zone Bypassing/Unbypassing

When a zone is bypassed, its detector is ignored by the system and does not generate an alarm when triggered.

To bypass or unbypass a zone:

1. From the Bypass Zones menu, select Bypass/Unbyp. [21].
2. Using the arrow buttons, scroll to the zone you want to bypass or unbypass.
3. Press ✓ to change the bypass status.
4. Press ✘; *Save Changes?* is displayed.
5. Press ✓ to confirm the changed bypass status.

To unbypass all zones:

1. From the Bypass Zones menu, select Unbypass All [22].
2. Press ✓; all zones are unbypassed

All bypassed zones will be automatically unbypassed when the system is disarmed.

A fire, gas detection or flood zone cannot be bypassed.

7.3. User Codes

The **CommPact** supports a variety of individual user codes. Each of these codes is four digits long. Most system functions require you to enter a valid user code.

The ability to perform a function is defined by your user code's authorization level. These authorization levels are pre-defined for each code as explained below.

Code 1: Master Code

The master code is the highest user authorization level. With the master code, you can edit all other user codes. Additionally, the master code grants access to the Event Log, and the Service menu.

The default master code is 1234. Change this code immediately after the system has been installed!

Codes 2-19: Controlled Codes

When you use a controlled user code for arming and disarming, the system notifies the monitoring service.

Codes 20-25: Non-controlled Codes

Non-controlled codes do not cause the system to send Arm/Disarm reports to the monitoring service. The system sends a Disarm report only if you use this code to disarm the system after an alarm occurrence.

Codes 26-27: Limited Codes

A limited code enables you to issue a code that is valid for one day only. This code automatically expires 24 hours after it has been programmed.

Code 28: Duress Code

The duress code is designed for situations where you are being forced to operate the system. This user code grants access to the selected operation, while sending a Duress event message to the monitoring service.

Code 29: Telecontrol Code

The Telecontrol code is designed to enable the user to perform a number of tasks via their telephone. Using this code, the user can call their system to arm and disarm the system, activate and deactivate PGM output, cancel the siren or establish Two-Way Audio communication.

Editing User Codes

User code editing is a feature that is available exclusively to the master code. To maintain a high level of security, keep all user codes confidential.

To edit a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to edit;
3. From the code's sub-menu, select Edit Code; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Edit the code.
5. Press ✓; the new code is stored in the memory.

If you enter a code that is identical to an existing user code, the Control System sounds an error tone and the new code is not accepted. 0000 is not a valid user code as this value is used to delete a user code.

Deleting User Codes

As an additional security measure, make certain that you delete any extra codes that are no longer required.

To delete a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to delete;
3. From the code's sub-menu, select Edit Code; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Enter 0000.
5. Press ✓; the code is deleted.

The master code cannot be deleted.

User Code Descriptors

Using the alphanumeric keypad on the front panel, you can edit the 16-character user code descriptors and enter the name or title of the users to whom the code is allocated.

To enter text, press a button repeatedly to scroll through the characters that appear on the button. For example, press *6MNO* to enter M, N, O, or 6 respectively. You can also use the 1 and 0 buttons to enter symbols. After you enter text, the cursor automatically moves to the next character. During descriptor editing, use the left SOS button to enter a space before the current character. Use the Right SOS button button to delete the current character.

To edit a user code descriptor:

1. From the main menu, select User Codes [4].
2. Select a code.
3. From the code's sub-menu, select Descriptor.
4. Edit the descriptor using the alphanumeric keypad.

7.4. Follow-Me

The Follow-Me feature is designed to notify the user that certain events have occurred. Notification is made by SMS to your cellular phone or by opening a two way audio channel.

If using the TWA Follow-Me feature, the audio channel is opened after alarm events only.

To edit the Follow-me number:

1. From the main menu, select Telephone #, Follow me # [5].
2. Enter a telephone number for Follow-Me communication. If using the SMS Follow-Me feature, this number must be for a cellular phone with the capability to receive SMS messages.

You may only access Follow-me programming if the protocol for Account 3 is programmed as SMS or TWA Follow-me.

7.5. Event Log

The event log records events that have occurred within your security system. When the log is full, the oldest events are automatically erased and are replaced by new events.

To view the event log:

1. From the Event Log menu, select View Log [61]; the most recent event is displayed.
   - Press the left SOS button to display the Time/Date stamp or the default descriptor on the second row of the display.
2. Use the arrow buttons to scroll through the events.
3. When you have finished viewing, press ✘to exit the log.

The event log displays the following information for each event:

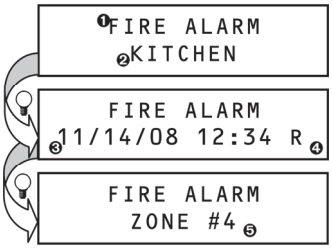
❶ The event – a brief description of the event that occurred.

❷ Zone descriptor – exactly where the event occurred.

❸ Time/date stamp – the exact time the event occurred.

❹ Report details – a single character indicating whether the event was reported to the central station. The options available are **R**: Report Sent, **F**: Report Failed, **N**: No Report, or **D**: Disabled.

❺ Default descriptor – zone number in this case



The above example shows the event log entry for a Fire alarm in the Kitchen (Zone 4) on November 14th 2008. The report was successfully reported to the central station.

7.6. Service Menu

The Service menu includes various functions that enable you to test your system effectively. You can gain access to the Service menu using the master code.

Set Time & Date

To set the time:

1. From the Service menu, select Set Time/Date, Set Time [7011].
2. Enter the current time.

To set the date:

1. From the Service menu, select Set Time/Date, Set Date [7012].
2. Enter the current date.

The format of time and date is defined by your installer in programming. If you are setting the time in 12hr format, use the left SOS button AM and PM.

Message Center

The Message Center is designed to allow you to record a short message that may be played back later by another user. After a message is recorded, *Message Waiting* is displayed on the LCD until the message is played back.

To play back a recorded message:

- From the Service menu, select Messages, Play Message [7021].

To record a message:

1. From the Service menu, select Messages, Record Message [7022].
2. Press ✓ to start recording the message.
3. Record your message. The message may be up to twenty seconds long.
4. Press ✓ to stop recording; the message is automatically played back and *OK?* is displayed.
5. Press ✓ to save your recording.

To delete a message:

1. From the Service menu, select Messages, Delete Message [7023]; *OK?* is displayed.
2. Press ✓; the message is deleted.

The Record and Play options can also be accessed via a convenient shortcut without needing to enter a valid user code.

To access the Record Message option from Standby mode, press ▲ then ✘.

To access the Play Message option from Standby mode, press ▲ then ✓.

Siren Tests

To test the external wireless siren:

- From the Service menu, select WL Siren Test [703]; the wireless siren is sounded briefly.

To test the built-in siren:

- From the Service menu, select Siren Test [704]; the built-in siren is sounded briefly.

Interface Test

The Interface test enables you to check if the speaker, LEDs and LCD are functioning correctly.

To test the system interface:

- From the Service menu, select Interface Test [705]; a short sequence of chimes are sounded from the speaker, all LEDs flash and the LCD is tested on all connected LCD keypads.

Walk Test

Walk Test mode enables you to test all the detectors registered to your system without triggering an alarm.

To initiate Walk Test mode:

1. From the Service menu, select Walk Test [706]; a list of registered detector appears.
2. Trigger each detector; when the system receives a successful transmission from a detector, the detector is removed from the list.
3. When all the detectors are removed from the list, End Walk Test is displayed.
4. Press ✘ to exit Walk Test mode.

Transmitters

The Transmitters menu offers two utilities, TX List and TX Test.

The TX List comprises all registered transmitters and their last reported status.

To view the TX list:

1. From the Service menu, select Transmitters, TX List [7071]; the first transmitter on the list is displayed.
2. Using the arrow buttons, scroll through the transmitter list.
3. When you have finished viewing, press ✘to exit the list.

The TX list and TX test display the following information on each transmitter:

1. The transmitter's Descriptor
2. The signal strength of the last received transmission
3. An abbreviation indicating the last received status of the transmitter

Status	Meaning	
OK	The transmitter is functioning correctly	
TA	Tamper condition	
BT	Battery low	Notify your installer
OS	The transmitter is out of synchronization	
NA	The transmitter is inactive	

Press The left SOS button

to display the transmitter's default descriptor.

The second utility, TX Test enables you to identify transmitters.

In TX Test mode, each time a transmission is received, a chime is sounded and the activated transmitter's details are displayed.

To initiate TX Test mode:

1. From the Service menu, select Transmitters, TX Test [7072].
2. Activate a transmitter; the transmitter's details are displayed.
3. When you have finished, press ✘to exit TX Test mode.

Audio Volume

To adjust the sensitivity of the microphone and the volume of the speaker:

1. Establish a two-way audio connection.
2. During the two-way audio session, from the Service menu, select Audio Volume [708].
3. Adjust the setting according to the following table.

Reading	Meaning
1	Increase microphone sensitivity
4	Reduce microphone sensitivity
3	Increase speaker volume
6	Reduce speaker volume

Display Version

To display the system's software version:

- From the Service menu, select Version [710]; the software (SW) is displayed.

Enable Programming

The installer or the Central Station are able to establish remote connection to the control system (using regular telephone, cellular communication, or through the Internet) in order to check the system status, program the control system, and change its settings.

If Installer Access is programmed as "user initiated" the installer or the Central Station cannot access the control system unless the Master User grants access with Enable Programming command.

To give access to programming:

- From the Service menu, select Enable Prog. [711]; a 30-minute time window is opened during which the Installer or RP gain access to the control system programming.

Global Chime

Each detector can be programmed by your installer to cause the system to chime when activated. This feature is active only when the system is disarmed. For example, the system can be programmed to sound a chime each time the front door is opened or closed. The Global Chime option enables you to turn this feature on and off.

To enable or disable Global Chime:

1. From the Service menu, select Global Chime [712].
2. Select either Enable or Disable.

Global Chime can also be accessed via a convenient shortcut without needing to enter a valid user code. To access the Global Chime option from Standby mode, press ▲ then ▼.

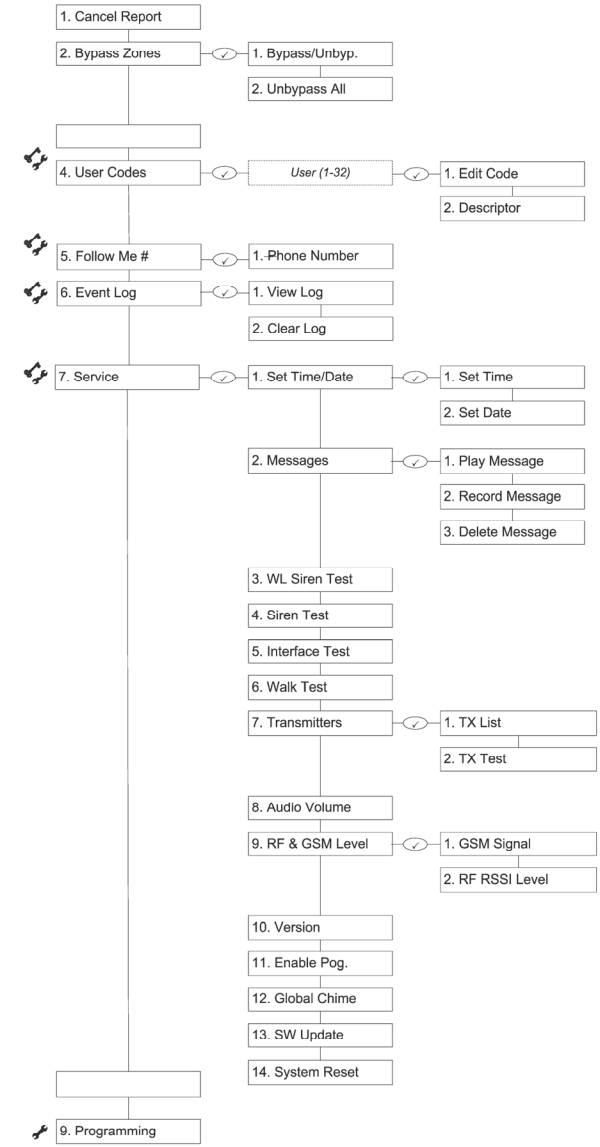
Remote Firmware Update

There is an option of control system software version update from a remote PC using WEB communication. If Remote Programming is programmed as "user initiated" such update cannot be made unless the Master User grants access to it with Remote Software Update command.

To give access to Remote Firmware Update:

- From the Service menu, select Software Update [713]; a 24-hours time window is opened during which the Remote Firmware Update may be performed.

Appendix A: Menu Structure



Legend:

Installer code required

Master code required

Appendix B: Web User Application

The **Web User Application - MyELAS** provides a full interface to your system from a local or remote PC. Via the Web you can perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control.

The **Smartphone Application - MyELAS** provides access to the Web User Application from your Smartphone (iPhone or Android).

Register to MyELAS

The Web Application is part of the service provider's Web site and requires the end user to register in order to gain access to the Web site.

To Register to MyELAS:

1. Go to www.MyELAS.com. The Login page is displayed.

Username:
Password:
Pass Code:
ENTER
English
Electronics Line 3000 Ltd provides innovative security with remote management solutions to the residential and commercial markets - built upon 20 years of technological leadership. Multiple technologies and applications are integrated to enable real-time data, audio and video solutions which are communicated via PSTN, GSM, GPRS and TCP/IP connections.
Everything is under control
Use this web application to perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control.
Control and schedule automated lights and appliances in your
Self Registration... | Password Recovery...

Figure 1: Login Page

If you have already registered but forgotten your Login details, click the Password Recovery link and you can request that the password to be sent to your predefined email address

2. Click the Self Registration link. The Self Registration page is displayed.

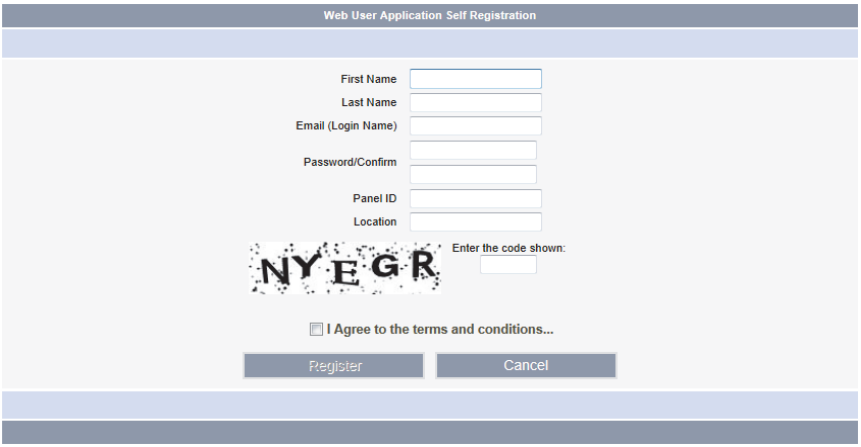


Figure 2: Self Registration Page

3. Enter the following registration details into the Self Registration page:

First/Last Name	Enter your First and Last Name
Email (Login Name)	Enter your chosen Login Name (i.e. email address)
Password/Confirm	Enter your chosen Password twice (minimum of 6 characters and at least one digit)
Panel ID	Enter your Panel ID (supplied by your service provider or as it appears on the sticker located on the side of the panel)
Location	Select your location time zone
Anti-Spam Code	Enter the displayed anti-spam code into this field
Terms and Conditions Agreement	Read the Terms and Conditions Agreement and check the checkbox to continue

4. Click Register. The Self Registration process sends a confirmation email to your specified email address.
5. From the received email, click the attached link to confirm your registration. The Login page is displayed and you can now login to the Web Application.

Login to MyELAS

To enter MyELAS:

1. Go to www.MyELAS.com. The Login page is displayed.

Username:
Password:
Pass Code:
ENTER
English
Electronics Line 3000 Ltd provides innovative security with remote management solutions to the residential and commercial markets - built upon 20 years of technological leadership. Multiple technologies and applications are integrated to enable real-time data, audio and video solutions which are communicated via PSTN, GSM, GPRS and TCP/IP connections.
Everything is under control
Use this web application to perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control.
Control and schedule automated lights and appliances in your
Self Registration... | Password Recovery...

Figure 3: Login Page

To login to the Web Application:

2. Enter your User Name and Password that you supplied during the registration process.
3. Enter your Pass Code (User Code) and click the Enter/Login button.

For your system security reasons, you must change the password immediately at first login. You can change your password on the Change Password page that is accessible from the Settings menu. Your new password should be no less than six characters and must start with a letter

You can also login to MyELAS using your Smartphone: Download the MyELAS app from the Apple App store or from Google play for Android devices.

When using the Smartphone application service, the Login page may look similar to the following examples:

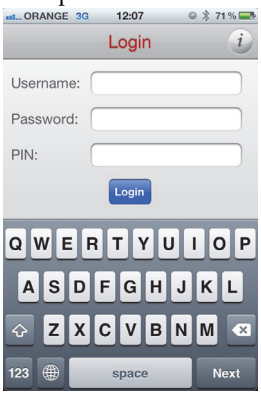


Figure 4: Login Page (iPhone)

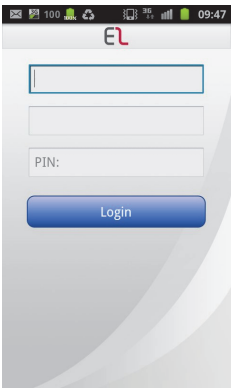


Figure 5: Login Page (Android)

The Main Page

After logging in, your system's home page is displayed. The following diagram shows the Main page and explains the main elements of the Web application's interface.

HOME
SET/UNSET
SETTINGS
HISTORY
VIDEO
Full Set
SET
LOG OFF
Help | Downloads | Contact Us
Set/Unset
Set and unset your control system remotely.
Settings
Manage different aspects of your control system and web user interface.
History
View a full list of system events that occurred in your home. Print or save the log file.
Omit Zones
Displays a list of the zones (i.e. sensors) in your system and allows you to omit or un-omit them.
Video
View images from PIR cameras or video streaming from IP cameras.
Alerts
Manage contacts for system event notification allowing you and your family to always stay informed.
See it all, control it all
Welcome to your web user application, a comprehensive interface to your home. The current status of your system is displayed in the status bar at the bottom of this page. Using this application, you can arm or disarm your system or select any of the functions listed above.
System status received at: 14/10/2012 12:39:50 (local time at control system)
Kobi Israeli Logged in
Unset
SYSTEM READY
REFRESH STATUS

Figure 6: Main Page

Menu Bar

The Menu Bar includes the Main Menu options as well as the Log Off button. The Main Menu offers the user links to various pages in the Web Application. Use the Logoff button on the right side of the menu to close the session.

The following options are available from the Main Menu:

- Home – pressing the Home button allows the user to return to the Home page at any time.
- Arm/Disarm – provides access to the System Operation Area page.
- Settings – offers various options including user code and contact management, event log viewing and zone bypass.
- History – enables you to view the system's event log.
- Video – You can discuss the home automation capability with your security service provider to determine if it is applicable to your system.
- Automation – You can discuss the home automation capability with your security service provider to determine if it is applicable to your system.
- Help/Download – offers online explanations on how to use the Web Application plus FAQ and customer support options.

Status Bar

The Status bar displays information on your system's status and the name of the user currently logged in. Above the status bar, the time when the system status display was last updated is shown. This information is displayed according to the local time at the control system. The system status refreshes automatically, and can also be refreshed manually. To refresh the current system status, click the Refresh Status button on the right-hand side of the Status bar.

Workspace

The workspace offers additional links to the following pages of the application: System Operation, Settings, History, Video and Automation. When you choose a page, either from the Main Menu, or from the workspace, the page is displayed in the workspace. For example, if you choose Arm/Disarm from the Main Menu, System Operation Area page and System Status area are displayed in the workspace (see the example below).

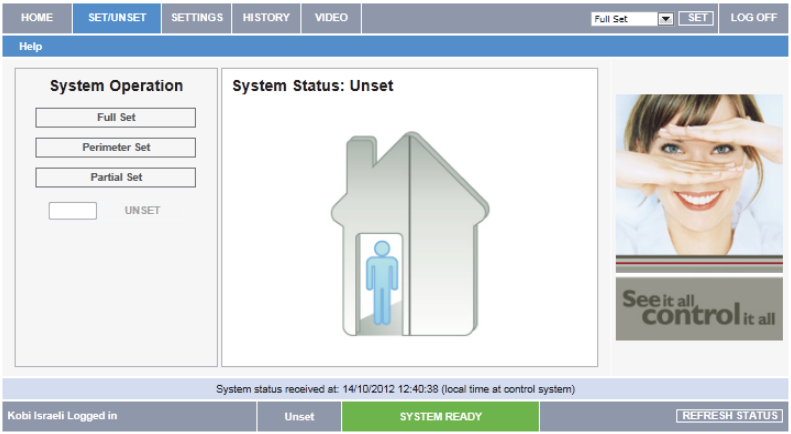


Figure 7: Workspace Example Page

You can arm and disarm the system using the Arm/Disarm drop-down box (upper-right part of the page) or using the buttons in the System Operation Area.

- The Web Application allows you to arm and disarm your system using any of the available arming methods.
- On the Status Bar below on the page you can see the current status of the system (in our example it is Disarmed and System Ready, which means that the system and all the detectors are working properly and there are no events to report). It is possible to check if there were alarms in the system.

It is important to note that when you are using the Web application, the system is armed with the programmed delay

Home Button

Press the Home button on the Main menu to return to the Main page at any time.

Arming and Disarming

Arming can be defined as turning the system on. When the system is armed, it monitors the zones that are protected by the detectors. If a detector detects an intrusion, the system generates an alarm. Certain detectors can be programmed by your installer to be active 24 hours a day. These detectors are always active regardless of system status.

To display the System Operation Area page:

On the Menu Bar, click Arm/Disarm. The System Operation page is displayed.

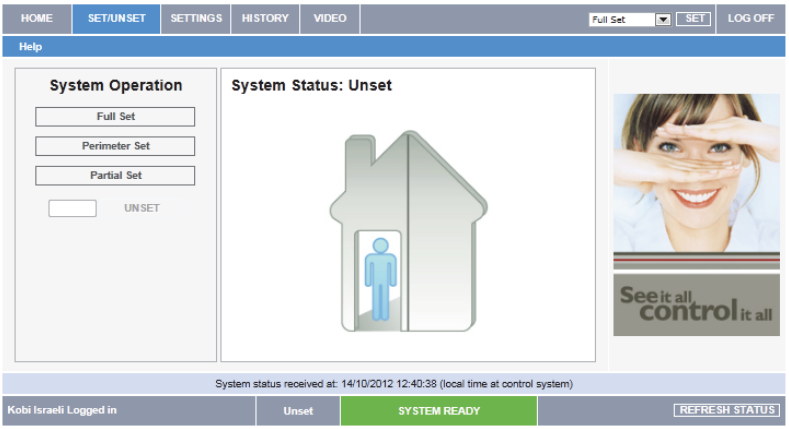


Figure 8: System Operation Area Page

Three arming modes are available: Away, Part and Perimeter. These modes enable you to arm your system accordingly to suit different circumstances.

Full Arming	Full Arming activates the entire system. This arming method is used when you intend to leave your home, leaving the premises empty.
Part Arming	Part Arming enables you to arm a section of your home while remaining on a different part of the premises. For example, at night your family is upstairs while the area downstairs is armed.
Perimeter Arming	Perimeter Arming enables you to turn on the perimeter zones (the windows and doors of your home) enabling you to move freely within the protected area.

Before arming the system, check that all doors and windows are closed so that the system is ready for arming. System status is displayed on the status bar at the bottom of the page. If you are arming from a remote location and the system status is "Not Ready", you may temporarily bypass any zone that is causing this condition.

Disarming can be regarded as turning the security system off. When the system is disarmed only zones that are defined as active 24 hours are monitored (e.g. Flood, Gas and Panic zones).

Web Application Settings

The Web Application Settings area offers various options including system/Web user codes, contact and password management, user interface appearance and descriptors, event log viewing and zone bypass capabilities.

System Users and Codes

The System Users and Codes page enables you to manage your system's users. The page displays a table of the system's current users and enables you add, edit and delete users as required.

This capability is available only to a user with a Master code, the highest level of authorization.

The System Users and Codes page provides a useful tool for managing your system's users. In this area you can add, delete, or change System Users and the User Codes for your system (for example, add/edit codes for family members).

The following System User types are available:

Master Code (Code 1)	The Master code is the highest user authorization level. With the Master code, you can change all other user codes.
Controlled Codes (Codes 2-19)	When you use a controlled user code for arming and disarming, the system notifies the monitoring service. You can assign these codes to your children or employees whose comings and goings are of interest to you.
Non-controlled Codes (Codes 20-25)	Non-controlled codes do not cause the system to send Arm/Disarm reports to the monitoring service. The system sends a Disarm report only if you use this code to disarm the system after an alarm occurrence.
Limited Codes (Codes 26-27)	A Limited code is a code that is valid for one day only. This code automatically expires 24 hours after it has been programmed. You can assign a limited code to a visiting guest, for example.
Duress Code (Code 28)	The Duress code is designed for situations where you are being forced to operate the system. This user code performs the operation selected, while sending a Duress event message to your monitoring service.

To display the System Users and Codes page:

1. On the Menu Bar, click Settings.
2. Click System Users and Codes. The System Users and Codes page is displayed.

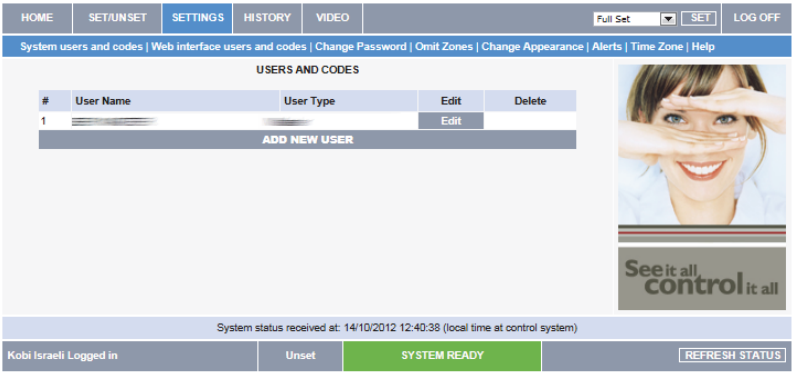


Figure 9: System Users and Codes Page

To add a new system user:

1. Click Add New User at the bottom of the table; the Add New System User page opens.

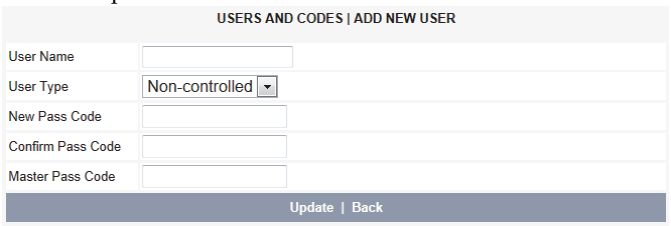


Figure 10: Add New System User Page

2. Enter the user's name in the field provided (16 characters max.).
3. Choose the user type from the available options.
4. Enter the new user's 4-digit passcode.
5. Enter the new user's passcode again for confirmation.
6. Enter your Master code.
7. Click Update.

To edit an existing system user:

1. Click Edit for the user you want to modify; the Edit User page opens.
2. Edit the user's name in the field provided (16 characters max.).

When editing an existing user, you cannot change the user type.

3. Enter the user's 4-digit passcode.
4. Enter the user's passcode again for confirmation.
5. Enter your Master code.
6. Click Update.

To delete a system user:

1. Click Delete for the user you want to remove from the table; the confirmation page opens.
2. Click Yes to confirm.

Web Interface Users and Codes

The Web Interface Users and Codes page enables you to manage your Web's users. The page displays a table of the system's current users and enables you add, edit and delete users as required. You can even issue temporary (limited) codes to guests that will automatically expire after 24 hours.

1. On the Menu Bar, click Settings.
2. Click Web Interface Users and Codes. The Web Interface Users and Codes page is displayed.

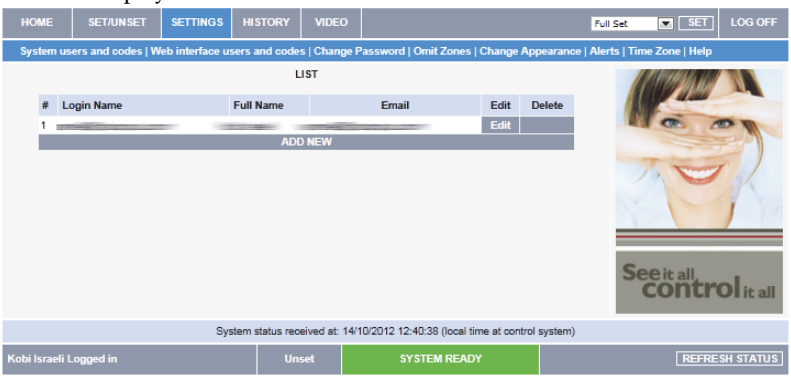


Figure 11: Web Interface Users and Codes Page

To add a new Web user:

1. Click Add New User at the bottom of the table; the Add New Web User page opens.

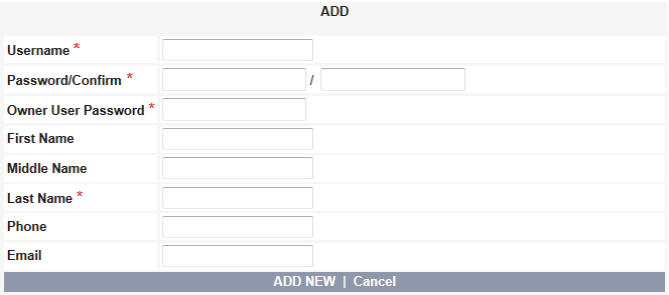


Figure 12: Add New Web User Page

2. Enter the user's name in the field provided (16 characters max.).
3. Enter the new user's password.
4. Enter the new user's password again for confirmation.

5. Enter the Owner User password.
6. Enter the First Name, Middle Name and Last Name of the new user in the fields provided.
7. Enter Phone and Email details of the new user into the fields provided.
8. Click Add New.

To edit an existing Web user:

1. Click Edit for the user you want to modify; the Edit User page opens.
2. Edit the user's name in the field provided (16 characters max.).
3. Enter the user's password.
4. Enter the user's password again for confirmation.
5. Enter the Owner User password.
6. Edit the First Name, Middle Name and Last Name of the user in the fields provided.
7. Edit the Phone and Email details of the user into the fields provided.
8. Click Update.

To delete a Web user:

1. Click Delete for the user you want to remove from the table; the confirmation page opens.
2. Click Yes to confirm.

Change Password

The Change Password page allows you to modify the password you use to log in to the Web Application.

To change the password:

1. On the Menu Bar, click Settings.
2. Click Change Password. The Change Password page is displayed.

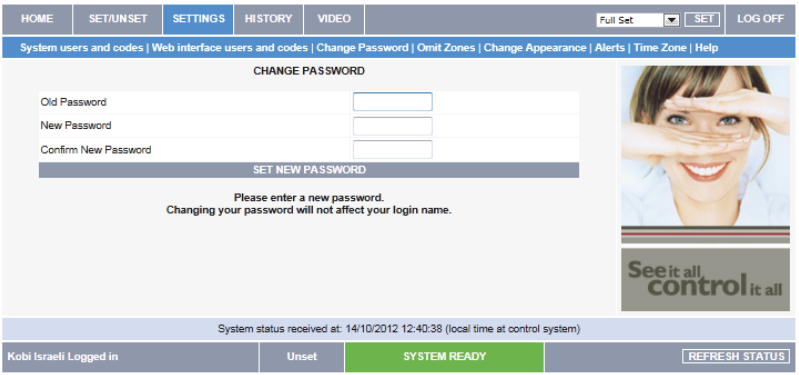

HOME
SET/UNSET
SETTINGS
HISTORY
VIDEO
Full Set
SET
LOG OFF
System users and codes | Web interface users and codes | Change Password | Omit Zones | Change Appearance | Alerts | Time Zone | Help
CHANGE PASSWORD
Old Password
New Password
Confirm New Password
SET NEW PASSWORD
Please enter a new password.
Changing your password will not affect your login name.
See it all, control it all
System status received at: 14/10/2012 12:40:38 (local time at control system)
Kobi Israeli Logged in
Unset
SYSTEM READY
REFRESH STATUS

Figure 13: Change Password Page

3. Enter the old password.
4. Enter a new password.

The new password should be no less than six characters and should start with a letter

5. Enter the new password again for confirmation.
6. Click Set New Password.

Zone Bypass

A bypassed zone is ignored by the system and does not generate an alarm when triggered. To "unbypass" a zone is to restore the zone, effectively instructing the system to monitor activity from that zone.

All bypassed zones are automatically unbypassed when the system is disarmed.

The Zone Bypass page displays a list of the zones (i.e. detectors) in your system and allows you to bypass or unbypass them as required.

To bypass a zone:

1. On the Menu Bar, click Settings.
2. Click Zone Bypass. The Zone Bypass page is displayed.

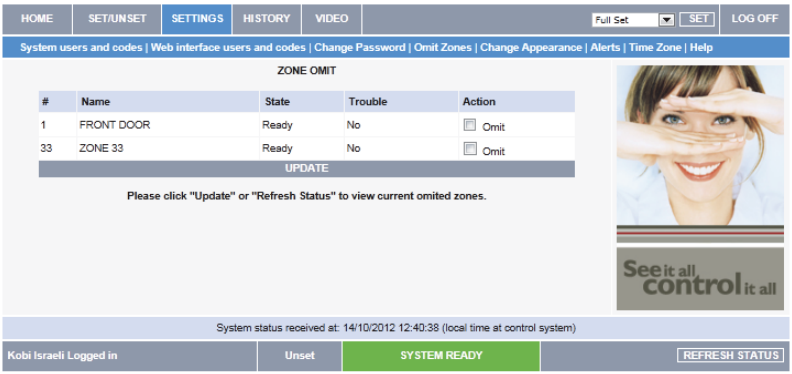

HOME
SET/UNSET
SETTINGS
HISTORY
VIDEO
Full Set
SET
LOG OFF
System users and codes | Web interface users and codes | Change Password | Omit Zones | Change Appearance | Alerts | Time Zone | Help
ZONE OMIT
Name State Trouble Action
1 FRONT DOOR Ready No Omit
33 ZONE 33 Ready No Omit
UPDATE
Please click "Update" or "Refresh Status" to view current omited zones.
See it all, control it all
System status received at: 14/10/2012 12:40:38 (local time at control system)
Kobi Israeli Logged in
Unset
SYSTEM READY
REFRESH STATUS

Figure 14: Zone Bypass Page

The table of zones displays your system's detectors and their current bypass status.

3. Check the checkboxes for the zones you want to bypass.
4. Click Update.

To restore a bypassed zone to normal operation, you can "unbypass" the zone.

Change Appearance

The Change Appearance page allows you to choose a color scheme for the interface of the Web Application.

To change the interface color scheme:

1. On the Menu Bar, click Settings.
2. Click Change Appearance. The Change Appearance page is displayed.

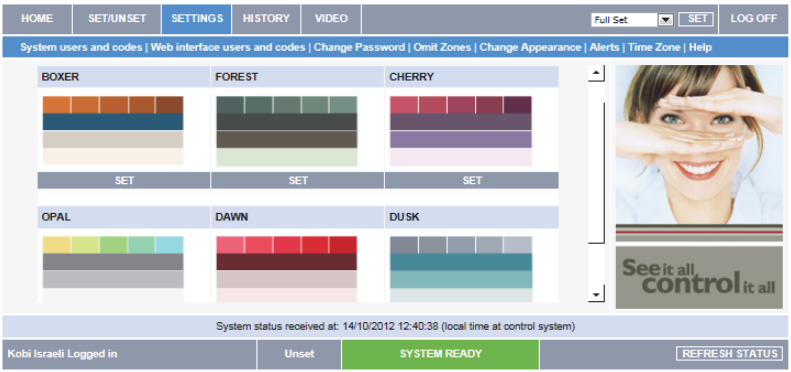


Figure 15: Change Appearance Page

3. Click "Set" underneath the required color scheme or "Set Default" to restore the default color scheme.

Alerts

The Alerts feature allows those people included in your contact list to be notified by email or SMS when certain events occur. The page displays a table of the system's alert contacts and enables you add, edit, test and delete contacts as required.

To display the Alerts page:

1. On the Menu Bar, click Settings.
2. Click Alerts. The Alerts page is displayed.

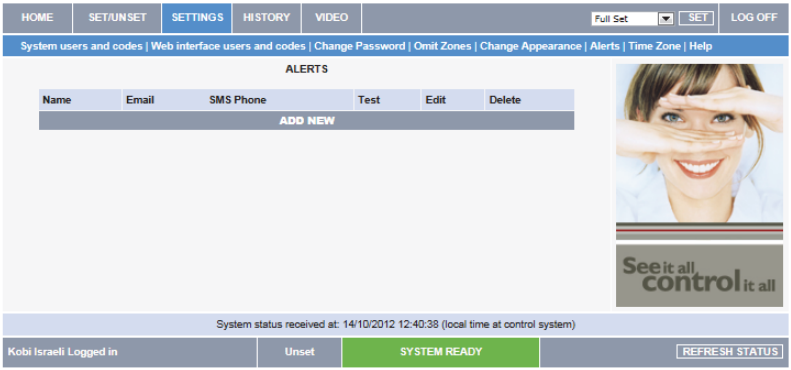


Figure 16: Alerts Page

To add new alert contact:

1. Click Add New at the bottom of the table; the Add New Alert Contact page opens.

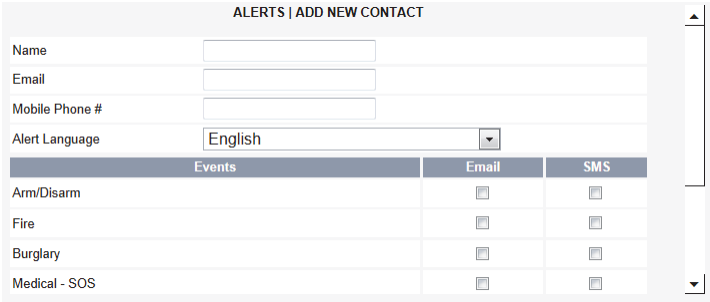


Figure 17: Add New Alert Contact Page

2. Enter the contact's name in the field provided.
3. Enter the new contact's email address.
4. Enter the new contact's mobile phone number
5. Select the alert language from the available list.
6. Choose the event and message type from the available options (Email, SMS).
7. Click Update.

To send a test message:

1. Click Test for the contact to whom you want to send a test message; a confirmation page appears.
2. Click OK.

To edit an existing alert contact:

1. Click Edit for the contact you want to modify; the Edit Alert Contact page opens.
2. Edit the contact name, email address and mobile number as required.
3. Choose the event and message type from the available options (Email, SMS).
4. Click Update.

To deleting an alert contact:

5. Click Delete for the contact you want to remove from the table; the confirmation page opens.
6. Click Yes to confirm.

Time Zone

The Time Zone page allows you to define the time zone for the control panel.

To display the Time Zone page:

1. On the Menu Bar, click Settings.
2. Click Time Zone. The Time Zone page is displayed.

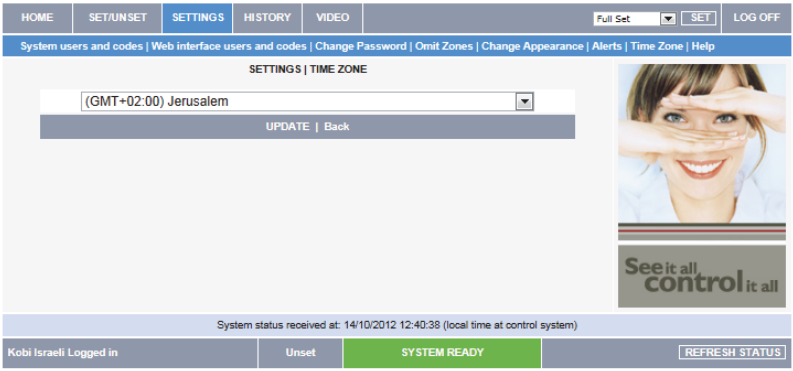


Figure 18: Time Zone Page

3. Choose the applicable time zone from the available options.
4. Click Update.

Event Log History

The Event Log History page displays a log of events that have occurred within your system. For each event you can view the date and time that the event occurred, a description of the event, the user or device that caused the event and whether or not the event was reported to your monitoring service. In addition to viewing the event log, you can also save the log to a pre-formatted file or simply print the log.

To view the event log history:

On the Menu Bar, click History, the Event Log History Page is displayed:

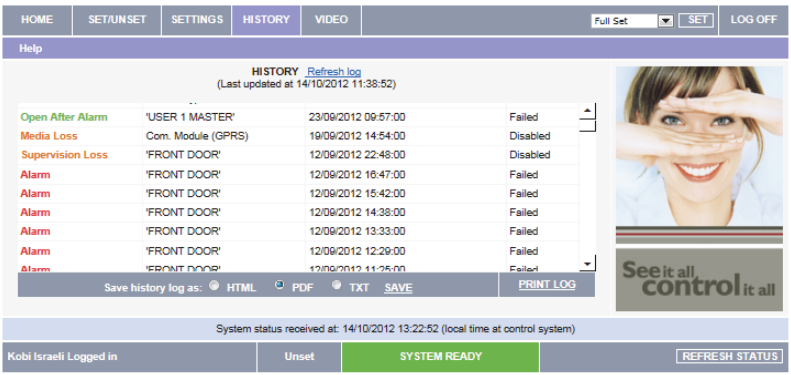

HOME
SET/UNSET
SETTINGS
HISTORY
VIDEO
Full Set
SET
LOG OFF
Help
HISTORY Refresh log
(Last updated at 14/10/2012 11:38:52)
Open After Alarm 'USER 1 MASTER' 23/09/2012 09:57:00 Failed
Media Loss Com. Module (GPRS) 19/09/2012 14:54:00 Disabled
Supervision Loss 'FRONT DOOR' 12/09/2012 22:48:00 Disabled
Alarm 'FRONT DOOR' 12/09/2012 16:47:00 Failed
Alarm 'FRONT DOOR' 12/09/2012 15:42:00 Failed
Alarm 'FRONT DOOR' 12/09/2012 14:38:00 Failed
Alarm 'FRONT DOOR' 12/09/2012 13:33:00 Failed
Alarm 'FRONT DOOR' 12/09/2012 12:29:00 Failed
Save history log as: HTML PDF TXT SAVE
PRINT LOG
See it all, control it all
System status received at: 14/10/2012 13:22:52 (local time at control system)
Kobi Israeli Logged in
Unset
SYSTEM READY
REFRESH STATUS

Figure 19: Event Log History Page

To save the event log:

Select the type of file you want to save (HTML, PDF or RTF) and click Save.

To print the event log:

Click Print Log (located in the bottom right hand corner underneath the event log table).

Appendix C: Glossary

24hr Zone — A detector which is always active regardless of whether the system is armed or disarmed.

A

Armed — The state during which the security system is activated. In most cases, when the system is armed, triggering a detector generates an alarm.

Arming Keys — The three keys on the front panel or keypad that activate one of the system's arming options.

B

Bypassed Zone — A detector which is ignored by the system. No alarm is generated from a bypassed zone even if triggered when the system is armed.

C

Cancel Key — A key on the Wireless Keypad that causes the system to disregard any partially entered code or command that may have mistakenly been entered.

Cancel Report — An operation that clears all communication buffers and stops the transmission of any pending messages to the monitoring service.

Cellular Communication — Monitoring and control via a cellular network.

Chime — A feature that provides audible annunciation when specific detectors are activated.

Code — See User Code

Controlled Code — A user code that causes the system to notify the monitoring service when used to arm or disarm.

D

Delay — The exit/entry delay times that allow the user to arm or disarm the system without generating an alarm.

Descriptor — Custom labels programmed for each user code, zone, keyfob, keypad etc.

Disarmed — The state during which the security system is deactivated. During disarm only detectors that are defined as 24hr, Panic, Medical, Fire, Gas, Flood and Environmental are capable of generating an alarm.

Detectors — The devices installed around the home that alert the panel in the event of an alarm.

Duress Code — A user code that generates a silent alarm to indicate that the user is being forced to operate the system.

E

Entry Delay — See Delay

Event Log — A browsable record of events that have occurred within the system.

Exit Delay — See Delay

F

Follow-me — A feature that enables users to receive notification to their telephone that an event has occurred in the system.

Forced Arming — Arming before the system is ready. If the system is not secured by the time that the exit delay expires, an alarm is generated.

Front Panel — The main interface located on the front of the Control System consisting of an LCD keypad.

Full Arming — An arming method that activates the entire system when the premises are vacated.

G

Global Chime — A feature that enables/disables the Chime feature for the entire system – see Chime.

I

Instant Arm — An arming method that cancels the entry delay after the system has been Part or Perimeter armed.

K

Keyfob — Handheld wireless transmitters used to remotely control the system.

L

LAN IP Address — The address that your home router has assigned to the Control System.

Limited Code — A user code that automatically expires 24 hours after it is programmed.

Log — See Event Log

M

Master Code — The only user code with the ability to program other user codes. The master code also has exclusive access to specific system functions.

Medical Emergency — A type of alarm that informs the monitoring service that the user is in need of medical assistance.

Message Center — An optional feature that enables users to record messages to be played back by other users.

N

Non-Controlled Code — A user code that does not cause the system to notify the monitoring service when used to arm or disarm. The system only reports if the code is used to disarm after an alarm.

O

One-Key Arming — Arming the system without the need for a valid user code.

P

Panic Alarm — A user initiated event that alerts the monitoring service in the event of an emergency.

Part Arming — An arming method that is designed to activate a certain section of the premises.

Perimeter Arming — An arming method that is designed to activate the detectors protecting the doors and windows while enabling residents to move freely on the premises.

PGM — Programmable output that is triggered according to specific system status conditions, or by remote command sent via PSTN, GSM, Ethernet, keyfob, keypad, or Remote Programmer.

R

Ready — The state in which all zones are closed and the system is ready to be armed.

Remote Firmware Update — Control System's firmware update from a remote PC using WEB communication.

Restore — Restore of the normal state when the trouble is repaired. For example, if AC power is reconnected, an AC Loss Restore event code is sent to the central station.

S

Service Call — A feature that enables the user to contact the monitoring service and talk to an operator via the Control System.

SMS Command — An SMS message sent to the Control System that causes the system to perform a specific function.

SMS Confirmation — An SMS message sent to the user confirming that the SMS command has been performed.

System Status LEDs — Luminous indicators on the front panel that provide information on the arm and power status of the system.

T

Telecontrol — A feature that provides remote access via the telephone including remote arming/disarming, siren cancel and Two-Way audio.

Tones — Chimes sounded by the Control System's internal or external siren.

Trouble Tones — Tones sounded by the system to indicate a trouble condition.

TWA — Two-Way Audio (abbr.)

TX — Transmitter (abbr.)

TX List — A service feature that lists all the system's registered transmitters, their last recorded status and signal strength.

TX Test — A service feature that displays the source of the last received transmission.

U

Unbypass — The restore of original state to a bypassed zone.

User Code — A four-digit code that grants access to certain system functions such as arming and disarming the system.

W

Walk Test — A mode that enables detectors to be tested without generating an alarm.

WUAPP — Web User Application Interface (abbr.) Web Application allowing full interface to the system's user functions.

WAP — A protocol used to enable access to the mobile Web via mobile phone or PDA.

Web Remote Programmer — Software that enable installers or service providers to operate and program the system from a PC either on-site or from a remote location.

Z

Zone — A protected area within the security system.

Zone Bypassing — See Bypassed Zone

Electronics Line 3000 Ltd. Limited Warranty

EL and its subsidiaries and affiliates ("Seller") warrants its products to be free from defects in materials and workmanship under normal use for 24 months from the date of production. Because Seller does not install or connect the product and because the product may be used in conjunction with products not manufactured by the Seller, Seller can not guarantee the performance of the security system which uses this product. Sellers' obligation and liability under this warranty is expressly limited to repairing and replacing, at Sellers option, within a reasonable time after the date of delivery, any product not meeting the specifications. Seller makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. In no case shall seller be liable for any consequential or incidental damages for breach of this or any other warranty, expressed or implied, or upon any other basis of liability whatsoever. Sellers obligation under this warranty shall not include any transportation charges or costs of installation or any liability for direct, indirect, or not be compromised or circumvented; that the product will prevent any persona; injury or property loss by intruder, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. Buyer understands that a properly installed and maintained alarm may only reduce the risk of intruder, robbery or fire without warning, but is not insurance or a guaranty that such will not occur or that there will be no personal injury or property loss as a result. Consequently seller shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning. However, if seller is held liable, whether directly or indirectly, for any loss or damage arising from under this limited warranty or otherwise, regardless of cause or origin, sellers maximum liability shall not exceed the purchase price of the product, which shall be complete and exclusive remedy against seller. No employee or representative of Seller is authorized to change this warranty in any way or grant any other warranty.

WARNING: This product should be tested at least once a week.

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to local regulations.

Contacting Electronics Line 3000 Ltd.

UPGRADING
EVERYDAY
SECURITY

CE

International Headquarters:
Electronics Line 3000 Ltd.
14 Hachoma St., 75655
Rishon Le Zion, Israel
Tel: (+972-3) 963-7777
Fax: (+972-3) 961-6584

All rights reserved.
No part of this document may be reproduced in any form without prior written permission from the publisher.